IAC-11.D6.1.6

THE FIRST FLIGHT DECISION FOR NEW HUMAN SPACECRAFT VEHICLES - A GENERAL APPROACH

Dawn M. Schaible
Systems Engineering Office Manager, NASA Engineering and Safety Center,
NASA Langley Research Center, Hampton, VA, USA
Dawn.M.Schaible@nasa.gov

John Phillip Sumrall*

Determining when it is safe to fly a crew on a launch vehicle/spacecraft for the first time, especially when the test flight is a part of the overall system certification process, has long been a challenge for program decision makers. The decision on first flight is ultimately the judgment of the program and agency management in conjunction with the design and operations team. To aid in this decision process, a NASA team undertook the task to develop a generic framework for evaluating whether any given program or commercial provider has sufficiently complete and balanced plans in place to allow crewmembers to safely fly on human spaceflight systems for the first time. It was the team's goal to establish a generic framework that could easily be applied to any new system, although the system design and intended mission would require specific assessment.

Historical data shows that there are multiple approaches that have been successful in first flight with crew. These approaches have always been tailored to the specific system design, mission objectives, and launch environment. Because specific approaches may vary significantly between different system designs and situations, prescriptive instructions or thorough checklists cannot be provided ahead of time. There are, however, certain general approaches that should be applied in thinking through the decision for first flight.

This paper addresses some of the most important factors to consider when developing a new system or evaluating an existing system for whether or not it is safe to fly humans to/from space. In the simplest terms, it is time to fly crew for the first time when it is safe to do so and the benefit of the crewed flight is greater than the residual risk. This is rarely a straight-forward decision. The paper describes the need for experience, sound judgment, close involvement of the technical and management teams, and established decision processes. In addition, the underlying level of confidence the manager has in making the decision will also be discussed. By applying the outlined thought processes and approaches to a specific design, test program and mission objectives, a project team will be better able to focus the debate and discussion on critical areas for consideration and added scrutiny – allowing decision makers to adequately address the first crewed flight decision.

* Advanced Development Office, Space Launch System Program Office, Marshall Space Flight Center, AL, USA

I. INTRODUCTION

Historical data shows that there are multiple approaches that have been successful for determining readiness for the first crewed flight. Every approach has to be tailored to the specific system design and situation of that particular system and mission objectives. Because specific approaches may vary significantly between different system designs, prescriptive instructions or thorough checklists cannot be developed to apply to all possible human spacecraft systems. There are, however, certain guiding principles that should be applied when developing the first crewed flight decision.

The NASA Engineering and Safety Center (NESC) developed a generic framework for evaluating whether any given program has sufficiently complete and balanced plans in place to allow crewmembers to fly safely on a human spaceflight system for the first time (i.e., first crewed flight). This framework, presented here, includes important factors to consider when developing a new system or evaluating an existing system for the first crewed flight. By applying the following framework to a specific design, test program, and intended mission objectives, decision makers will have better information with which to make the decision for first crewed flight.

The question of when to fly crew for the first time is evaluated at many stages through the development of the human spaceflight system—first during the planning stages and then throughout development and testing and at major milestones. In general terms, the system is ready to fly when residual risk[†] has been mitigated to the point where it is outweighed by the need to fly the first crew. This is rarely a straight-forward, clear-cut trade off so experience, sound judgment, and established (and clearly documented) decision-making processes are essential. In addition, the underlying level of confidence the manager has in making the decision must be considered.

The decision on first flight is ultimately the judgment of the program and Agency management in conjunction with the design and operations team. There is, however, some general guidance that can be used in making these judgments. Close involvement of the technical and management teams throughout the design and development process is essential. Verification and validation (V&V) of safety-critical systems and survival functions are required. Based on previous experience, historical perspectives, and best practices, this paper will illustrate a top-level thought process for making a first flight decision and will help focus the debate and discussion on critical areas for consideration and additional scrutiny.

II. NEED FOR FIRST CREWED FLIGHT

Given that the human spaceflight system is designed for human spaceflight, it is accepted that the objective is to fly humans when risks to crew safety have been mitigated to the point where the need or benefit is worth the residual risks. The effort then shifts to deciding WHEN it is safe to fly crew, not IF a crew should fly.

Senior leaders and decision makers must evaluate the specific test objectives for the mission to determine the need for a crew. Once this need has been established, the focus then shifts to ensuring that the necessary safety-related crew interface, safety, and survivability requirements are met. A prerequisite for a first crewed flight is confidence gained through understanding of the system design, development, analysis, and testing. It should be noted that the decision that crew is needed for a particular test or mission is primarily a programmatic decision (program and Agency management). For the technical team, the focus must be on ensuring a safe and technically sound system.

III. UNDERSTANDING AND MITIGATING RESIDUAL RISK

III.I Focus on Crew Safety

The process of designing, developing, and testing a new launch system is very complex and involves the spacecraft, launch vehicle, ground systems, mission systems, recovery systems, ground crews, and flight test crews. The program teams have a wide-ranging responsibility to ensure the system is adequately assessed, tested, and deemed safe for human flight. It is recognized that, despite the best efforts of the

[†] In this paper, residual risk is defined as the risk remaining after other known risks have been eliminated, managed, mitigated, or accepted

vehicle team, early flights of new systems will entail some degree of residual risk. Therefore, the focus should be on reducing and managing safety-related risk to the greatest extent practical. Initial crewed missions must be conducted with a minimum of onboard personnel (either active or passive participants). Such flights may warrant unique contingency procedures/capabilities that will preserve a safe return capability (i.e., above and beyond that required for the nominal design mission) utilizing specially trained crews.

In order to focus to those items that are unique to the initial crew participation, it is assumed the system/operations design must preserve a safe return to Earth capability in the presence of any single failure in any critical functional capability to the maximum extent practical. Safety issues, including providing for a safe crew return, should be separated from those needed only to enhance the mission. Mission enhancement functions of the crew are only considered to the extent that they affect safety. Figure 1 illustrates this concept. Safety and crew survival (such as abort capability) functions are non-negotiable and must be fully tested, verified, and validate prior to the first crewed flight. For each specific test or mission, additional functions will be required to meet objectives that have been defined. Each subsequent test and mission may require additional capability.

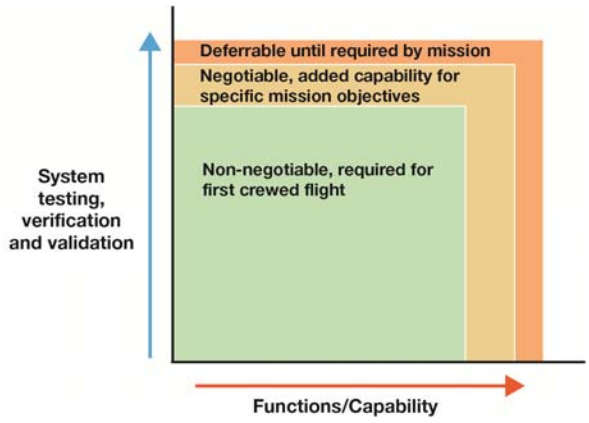

Figure 1: Focus on Safety-related Items and Risks

Functions that are critical for crew safety and survival must be established early in the design and development process. These crew safety and survival functions should be formed into a set of non-negotiable, first crewed flight requirements that form the basis for required design, development, testing, and V&V. The following criterion is assumed as the basis for determining the minimum requirements that must be satisfied in allowing crew participation: *System/operations design must preserve a safe return to Earth capability in the presence of any single credible failure in any critical functional path for the intended mission.*

The focus then shifts to determining what these safety-critical functions are and the degree to which they can be validated[‡].

III.II System Knowledge and Uncertainty Reduction

Safety must be an inherent part of the design. Programs must establish requirements for each system's specific design that will address safety-related items (e.g., failure tolerance, risk of loss of crew and mission, overall system reliability). A system-level focus on selection of simple and safe solutions to meet critical functions necessary to accomplish the mission is required. These safety-critical design requirements must be addressed prior to the first crewed flight. Sound aerospace-engineering practices for design, testing, and analysis must include all disciplines that affect any aspect of a safe design. Examples include: propulsion; environmental control and life support; structures; mechanisms; materials; active/passive thermal; pyrotechnics; aerodynamics; flight mechanics; loads and dynamics; guidance, navigation, and control; electrical systems; avionics; software; thermal protection; crew systems; human factors; communication; space environments; ground operations; and flight operations. In addition, design guidelines and standards associated with each technical and operational discipline must be considered relative to their effect on crew safety (e.g., margins, structural strength, and factors of safety). Including representation from those organizations that will operate the system (in flight and on the ground) is also important in the design of active

[‡] Verification of a product shows proof of compliance with requirements. Validation of a product shows that the product accomplishes the intended purpose—and in the case of models/analysis, that models adequately predict the environment and match actual vehicle performance.

systems and user interfaces, as well as during system-level testing.

Gaining understanding of system design, operation, and performance (hence reducing risk) is traditionally accomplished through many factors that have been established as part of sound engineering practices. Figure 2 highlights areas that warrant particular attention when determining first crewed flight readiness.

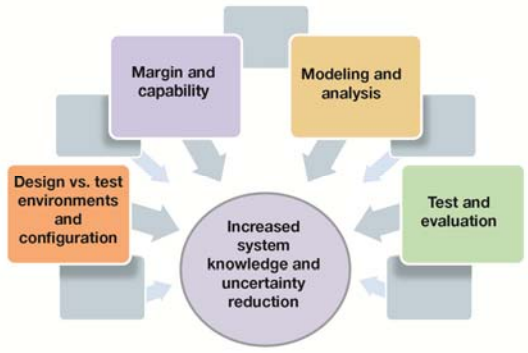

Figure 2: Major Contributors to Understanding Residual Risk for First Crewed Flight

Given that the first crewed flight is likely to occur as part of the development process, extra consideration for crew safety must be given to the specific mission plan and vehicle configuration. The flight test environment must be compared to previous test conditions/parameters and analysis assumptions. Understanding the environment in which the system will operate and how it will vary for different phases of the mission allows the system to be tested in relevant conditions and thus reduces uncertainty. Design and analysis should address full flight envelope operation of the spaceflight system's design capability (including induced and natural environments) and failure/abort conditions. Examples: loads analyses for launch, ascent, orbit, entry, and landing (coupled loads analyses); strength/stress/margin assessments for critical load conditions; entry heating and thermal protection system performance; crew life support; propulsion systems; and trajectories.

The flight hardware/software for test flights may, however, be in a different configuration than for operational flights, or may not be fully qualified. It is imperative that these differences be identified and thoroughly evaluated to fully understand the residual risk. The key areas that require specific attention and scrutiny include:

- Configuration of the vehicle for flight test versus previous tests
- Fidelity, assumptions, and validation of models versus flight configuration
- Analyzed configuration versus flight configuration
- Certification level and fidelity of hardware/software installed for flight test

A review of the specific flight configuration should be conducted, along with the implications of test results and anomaly resolutions from previous testing and analyses. Specific analyses may be performed for the mission, to include any potential contingencies. It is critical, however, to understand the assumptions and fidelity of the models being used, and where the results are valid for that particular flight configuration. Accepting data from models that are not validated within the range of operation can be problematic.

Another area that poses a potential problem for a first crewed flight is the certification level or fidelity of hardware/software installed on the vehicle for that flight (and of the ground systems used to support and operate the vehicle/mission). Due to timing and the requirements for the specific mission, engineering and/or prototype equipment may be used. Additional test instrumentation may also be part of the mission configuration. A decision to use an uncertified or off-nominal configuration requires a thorough review, including an assessment of any possible unintended interactions.

Managing margins is critical to the vehicle design and development. In this case, a margin is the difference between the design requirements (including factors of safety) and the system's actual performance capability in the worst-case environment and operating states. Examples of areas where margins are important include power, mass, delta-velocity, structure, and many others. Decision makers must understand the margins of each system before making a first flight decision. Planned operations are often placarded to stay within system capabilities, especially in the early development flights (in some cases, such as launch, it is difficult to

gain margin via placards; propulsion systems may operate near maximum levels on every mission). Through effective testing and proper processing, the actual system capability can be determined. Each development flight test provides increased knowledge and reduces uncertainty within the cleared envelope of operation—allowing for incremental envelope expansion as more measurements are obtained and analytical tools are validated. Figure 3 illustrates this concept. The outer oval represents the operational system capability or "designed to" envelope, as built up/validated over the course of the test program. A robust, reliable, and safe design incorporates the ability to test specific points of the design where lower margins, high risk, etc., occur due to new technology, use of previous technology in an untested environment, or other factors. As in most systems, the amount of margin varies. In some cases the system is quite robust (i.e., large positive margin), in other areas there is very little margin (see Figure 3). Greater margins are required where there is large uncertainty in the design and environments. Understanding the margins, to the maximum extent practical, is vital in determining the safety of first crewed flight.

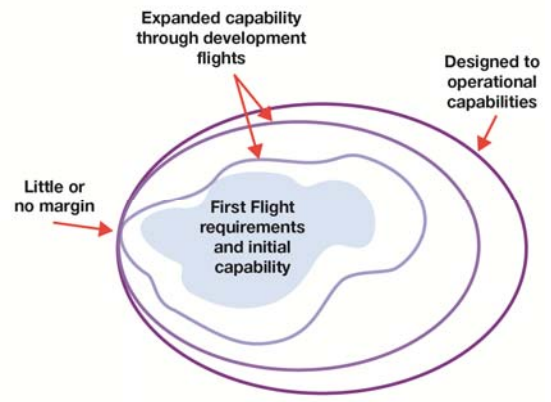

Figure 3: Understanding Margins and Incremental System Capability Validation

Minimizing risk goes beyond meeting requirements and adhering to established standards. It requires exploring what can go wrong and developing mitigations that either eliminate or reduce the ensuing residual risk to acceptable levels in the as-built system, including where uncertainties might reduce margins to unsafe levels along the flight envelope. Providing sufficient margin is an essential part of mitigating uncertainty and performing a safe mission.

Prior to crewed flight, the system's performance and operating margin relative to the natural and induced environments must be anchored by validated analysis/modeling and/or testing.

Knowledge of the design process improves understanding of the limitations of analysis techniques—as it is these limitations that are critical to understanding the risk and ultimately the safety of the system. The results from analytical tools are dependent on the accuracy of the models and the methods of calculation. While most results can be calculated to multiple significant figures, most models do not have that level of accuracy of the actual system/hardware. Many of the models may be approximations due to limited knowledge of the physics, external environment, systems, or limited resources. These tools have enormous potential for improving the development process once their results are validated by experimentation in each specific application. Furthermore, since these model formulations can be manipulated to match experimental data at a given condition, they cannot be considered accurate until the same formulation is used under multiple plausible conditions. Such validation can, to a large degree, be accomplished through ground testing, but there are several classes of measurements that can only be obtained with accuracy in flight (acoustics, aero-thermal, induced environments, etc.).

A ***critical test list*** is a key tool for determining when a vehicle is ready for flight. This list contains the tests, along with success criteria, that must be completed to reduce the system risk to an acceptable level and would cover the non-negotiable items. This list should be created early in the development process. While the overall test requirements will be fluid over the course of the program, changes to this critical test list should be rare and only done after much debate and agreement among the team. Adhering to the list will help guard against the pressures of limited resources (time and budget) that programs often face during development.

The progression from analysis to ground test and then to flight test (uncrewed and then crewed) is also the progression of the fidelity of data that can be generated. Ideally, safety-critical and survival functions would be tested and verified through ground tests. This is not always possible, as flight environments and potential interactions cannot

always be anticipated and replicated on the ground. Any safety-critical function that must operate (or must not operate) during a crewed mission must be verified and validated to an accepted confidence level prior to the first crewed flight. Flight and ground tests must have similar instrumentation and be in the same locations, as much as is practical, to compare data and allow the flight test to validate the ground test and the analysis. A single measurement in any of the testing may not be sufficient to validate the system or model.

To understand the uncertainty, and for the flight risk to be accepted, sufficient test measurements are needed to verify the environment, confirm the analysis, and confirm location of flight measurements. Flight tests should include: definition of flight test reference missions, objectives, flight-specific functions, performance, and verification requirements; and assessment of all waivers, deviations, and exceptions. Finally, the program should ensure the resolution of anomalies from previous ground and flight tests and identify deviations from previous tests and baseline design.

III.III Proven Means of Return to Earth

A safe return to Earth from any stage of a mission, including launch, must be ensured through contingency capabilities and procedures to the maximum practical extent. Careful thought must be given to the entire mission with the goal of always being able to return the crew safely to Earth. In addition, it must be verified that the intended mission can be controlled, with uncertainties, to remain within the flight envelope validated for that mission.

Launch through the atmosphere inherently poses a tightly constrained flight envelope due to the rapid release of large amounts of energy by the propulsion system, significant aerodynamic loading, and the fact that structural loads may be at their maximum for the launch vehicle and some spacecraft components. Therefore, early human spaceflight designs provided some form of “last resort” escape from the launch vehicle during the period from liftoff through maximum dynamic pressure (max q-bar), transonic transition, stage separation, and the establishment of a functioning upper stage. Because the range of unacceptable conditions is impossible to define with complete confidence, emergency system designs cannot ensure success in every conceivable case, but portions of the envelope can and must be verified and validated to be safe for supporting human flight. If a launch escape capability is available, it should not be factored into reliability considerations but serve as a last resort to preserve the life of the crew.

The Space Shuttle configuration, unlike the small crew capsules used in the early programs, precluded reliance on escape systems while its solid rocket boosters (SRBs) were burning. Because SRB thrust termination designs introduced additional safety risks, the design team elected to invest the resources necessary to provide assurance that the entire launch system could be treated, like primary structure, as having a reliability of 1.0 from ignition through SRB separation. The fact that an unrecognized combination of environments subsequently resulted in a catastrophe does not, by itself, invalidate the selected design approach. Rather, this tragic event reinforced the importance of meticulously monitoring flight and test data relentlessly pursuing, understanding, and resolving every out of family (not just out of specification) measurement.

Knowledge of the system and understanding of the residual risks are gained as a system evolves. Each step of the design, development, assembly, integration, and test process builds the body of evidence the decision makers can use to determine the acceptability of the residual risks. Therefore, the decision of first flight must be considered, planned, and assessed at each step of the process. An important part of this overall process is maintaining and encouraging the open discussions and debates within the entire program team—and maintaining a healthy tension between the program and technical authorities, operations and design, systems and disciplines, etc.

IV. CONFIDENCE

An important consideration in determining when it is safe to put crews in a human spaceflight system is the overall level of confidence that the decision makers have in the system. For this discussion the subjective confidence is based on engineering judgment, not statistical projections. Decision makers gain confidence through a combination of several tangible and intangible means. Some examples and

descriptions of contributing factors are provided in the following sections.

IV.I Design Maturity and Simplicity

The use of 'proven' hardware/software and designs can provide increased confidence, assuming similar environments, conditions, applications, etc. However, the design team should be cautious in using 'heritage' and 'off the shelf' hardware and software. The use of these proven systems must be analyzed and verified for use in new environments and applications. Designs that have additional safety margins at the component, system, or operations levels, as previously described, may also merit increased confidence.

Systems that employ inherently simpler designs, fewer interfaces, and large margins to meet their needs will likely increase confidence in their ability to perform safely and reliably. For example, the Space Shuttle drops its landing gear by releasing retention hooks and allowing gravity and air loads to deploy the landing gear, avoiding hydraulic or other actuating power devices. Complexity should only be added when there is benefit such as in weight, volume, performance, or operations.

IV.II Verification and Validation

V&V are essential for developing a safe human spaceflight system. When determining if a vehicle is ready for crewed flight, a review of the V&V program should be conducted. A complete and thorough test program will increase confidence in mission success. When a vehicle or system has a significant history of testing prior to the current program and the configuration, operational environment, and performance parameters are similar enough, the applicable historical test data and analyses may be used for verification and can also increase confidence in the system. Analytical design tools, validated with experimental data over a range of conditions, provide the most confidence.

The test program should always include end-to-end testing and integrate humans, hardware, and software to the degree needed to sufficiently understand the dynamics of interaction, control risk and gain confidence in the integrated system.

IV.III Program Team

The experience and longevity of the program team are significant confidence builders in development of a successful human spaceflight system.

Confidence is enhanced when program management and supporting members of the program team (such as Safety and Mission Assurance (S&MA) and Medical) are responsible for ensuring an appropriate emphasis on safety during the design, development, and testing of the launch vehicle, spacecraft, launch-abort system, mission operations, ground operations, manufacturing, and other areas.

Teams consisting of members with significant design/development experience in the fields they currently support and who have already been through major design, development, and testing campaigns provide increased confidence. A strong systems engineering focus is also important in understanding and managing the interfaces and interactions—of both the design and the team.

Confidence increases when decision makers insist on personal accountability (ownership) for the end results; good communication between team members; and operation in an open, positive environment. As stated earlier, maintaining and encouraging open discussions and debates within the entire team—and maintaining a healthy tension between the program and technical authorities, operations and design, systems and disciplines, etc., is an important part of developing confidence. Ideally, the team should be organized so that the decision-making authority is delegated to the hardware/system design level, thereby allowing timely decisions to be made. However, final accountability remains with the program and Agency managers. All decisions must consider safety first and be based on a balance of sound technical and programmatic rationale. It is important to note that organizations should have an alternate reporting path or governance structure that ensures safety and technical concerns are addressed.

It should be emphasized that hardware/software and system contractors are an essential part of the program team. The contract should allow open communication and individual responsibility. Since most hardware and software elements are provided by prime and sub-tier contractors, careful attention must be paid to the applicable statements of work,

terms, and conditions to make sure that they motivate all parties to ensure safety and reliability. Some contract incentives may drive behavior contrary to what is desired. A simplified example would be if all award fees are based on simply meeting milestones—schedule pressure could take precedence over technical matters.

IV.IV Program Processes

For any complex program, established, efficient, effective, and documented processes are essential to define how the program functions. Understanding and ensuring proper program processes and outcomes will help determine the level of confidence.

Examples of processes to be analyzed include technical reporting/authority, technical checks and balances, S&MA practices, integration, and documentation. For instance, decision makers may gain confidence when the team has clearly defined and understood roles and responsibilities; a strategy for independent reviews and reporting; well-established risk management practices that identify and eliminate, reduce, or mitigate risks; readily available and up-to-date documentation; and documented rationale of major decisions.

IV.V Demonstrated Record of Success

Human spaceflight systems typically have well-documented design processes, with thorough engineering standards and processes. Some systems, however, may offer limited access to detailed design information. These systems may have different design and verification approaches, as well as differing processes, documentation, or quality-control plans. From a confidence-building standpoint, these kinds of differences and potential shortcomings may well be offset, in part, by a demonstrated launch performance record. This concept may apply to complete human spaceflight systems, such as the Russian Soyuz, or components or subsystems, such as the RD-180 rocket engine.

An existing system or subsystem may add to the confidence of decision makers if it has established a sound flight record in a similar configuration or operation, or if it has undergone related systems testing. Successful components or systems may function or operate within specific parameters but if those components or systems are introduced into new parameters, their continued success cannot be assumed unless appropriate testing using these new parameters is performed. Decision makers should be cautious if components or systems that were successful in previous programs are now used in environments for which they were not designed or tested. In addition, understanding of all past anomalies is essential.

It is important to note that decision makers must remember that past success does not automatically translate to future success. Previous flight history is only one factor in building confidence - it is not sufficient by itself to determine readiness for a first crewed flight. When using these previously flown systems or components, it is vital that the technical team has a sound basis for confidence in their continued success. Every system will present its own unique set of circumstances that must be thoughtfully considered in a manner consistent with the principles described in this paper. In the end, the technical team will be accountable for the final results.

IV.VI Independent Input and Perspective

Throughout the process, program and Agency management should seek out and integrate input from competent, current, and independent review teams. It is important that they review the program throughout its life cycle and have relevant insight into and knowledge of the design in order to make sound observations and recommendations. However, care should be taken that the review team retains their independence and maintains a balance between close participation and independence. In addition, independent technical assessments of new technologies, new developments, and expected high-risk areas should be performed throughout the life cycle.

Confidence is not a number or a data point. Decision makers must develop confidence to safely launch humans by working closely with the entire program team throughout the process of designing, building, and testing the vehicle.

The factors outlined above, along with others, contribute to building confidence in the human spaceflight system's ability to fly a crew safely.

Overall confidence is a combination of many considerations and it is important that the contributing factors chosen encompass the entire system, including the launch vehicle and ground/mission systems. Readiness for crewed flight operations will always be an integrated judgment call based on the decision makers' experience, knowledge, and level of confidence in the system.

V. SUMMARY

The key points in this paper can be viewed as questions that a decision maker may ask throughout the process of designing, building, and testing a new crewed vehicle. Some of these questions include (but are not limited to):

- Are adequate safety features inherent in the design?
- Does the design preserve a safe return to Earth in the event of a single credible failure?
- Are the design requirements of the entire system understood and implemented?
- Does the team thoroughly understand the design and configuration?
- Has sufficient knowledge been gained through adequate design, analysis, and testing?
- Have models been thoroughly validated with physical data?
- Are hazards adequately identified and controlled, including across systems and interfaces, to the maximum extent practical?
- Have the safety-critical and survival functions been identified, verified and validated prior to the first crewed flight (including test flights)?
- Have the program management and technical teams worked together and has there been open communication of issues throughout the lifecycle?
- Has the first crewed flight decision been considered at each step of the lifecycle?
- Has confidence been developed throughout the lifecycle and used in making an informed judgment?
- When decisions were made, did the team focus on showing how those decisions affect overall safety and risk?
- Are the program, engineering, S&MA, and operations teams in agreement for system readiness of a first crewed flight?

The process of determining readiness for a first crewed flight is dependent on the specific system and mission. In general terms, the vehicle is ready to fly when it has been deemed safe and when any residual risk has been mitigated to the point that it is outweighed by the need for a crew. This decision is ultimately the judgment of the program and Agency management in conjunction with the design and operations team.

VI. SELECTED REFERENCES

NASA-TM-2011-217089, Readiness for First Crewed Flight

NASA-STD-3000, Man-Systems Integration Standards, July 1995

NPR 8705.2B, Human-Rating Requirements for Space Systems

T98-10212, A Review of Man Rating in past and Current Manned Space Flight Programs, A. Bond, 1998

SSP 30309E, Safety Analysis and Risk Assessment Requirements, July 2009

NPR 8000.4, Agency Risk Management Procedural Requirements, December 2008

7120.5D NASA Space Flight Program and Project Management Requirements

NASA SP-2007-6105, NASA Systems Engineering Handbook

NPR 7123.1A, NASA Systems Engineering Processes and Requirements